Guidelines for Evaluation and Testing of Non-Standard Equipment/Software

Commonwealth of Massachusetts
Criminal History Systems Board

Barry J. LaCroix
Executive Director

August 15, 2001

Table of Contents

1.0 Overview

The Criminal History Systems Board (CHSB) is charged by Massachusetts General Laws chapter 6, § 168 with the responsibility of providing for, and exercising control over, the installation, operation, and maintenance of data processing and data communications systems, referred to by said statute as the criminal offender record information system, or more commonly known within the Commonwealth and nationwide as the criminal justice information system (CJIS). The CHSB is further charged by statute with the responsibility for designing the CJIS so as to ensure the prompt collection, exchange, dissemination and distribution of information within that system as may be necessary for the efficient administration and operation of criminal justice agencies, as well as for connecting such system directly or indirectly with similar systems in this or other states.

A major consideration for the CHSB in modifying, expanding and/or testing the CJIS, or any of its components, is the security and integrity of the system. This policy statement is designed to optimize the CHSB's control of the system and to articulate the consequences if the system is compromised in any way.

2.0 General Purpose

2.1 It is the purpose of this document, pursuant to the authority delegated to the CHSB by M.G.L. c. 6, § 168, to establish guidelines to be used by the CHSB when dealing with outside vendors who wish to propose the use of equipment and/or software on the CJIS network.

2.2 It is the policy of the CHSB, as well as a requirement of the CJIS User Agreement (Section IV (D), Operational Responsibilities of User Agencies: Equipment and Maintenance), that only approved equipment may be connected to the CJIS network. Furthermore it is a requirement of this agency that said equipment and associated maintenance services may only be purchased from vendors approved by the CHSB.

2.3 The agency recognizes that there may be specific instances where functionality desired by members of our user community is not, or can not be provided by "standard" previously approved equipment. It is the purpose of these guidelines to provide a structure within which the staff of the CHSB will work with vendors to evaluate new types of hardware and software that the user community is interested in obtaining, but which deviates from currently approved and utilized equipment.

2.4 The agency will evaluate proposals from vendors when a user agency has expressed an interest in the technologies proposed by a vendor, and when the CHSB believes that the benefits of the proposed equipment/software would be of interest to multiple user agencies.

2.5 The Executive Director of the CHSB reserves the right to deny or delay the processing of requests under these guidelines based upon technical staff availability or in consideration of other priorities within the CHSB.

3.0 Proposed Technical Scope of Functionality

Any party interested in proposing equipment and/or software to be used with the CJIS shall submit to the CHSB a proposed technical scope of functionality, which shall include the following information:

3.1 The name, address, and phone number of the vendor, along with the name of the individual within the vendor organization that is assigned to work with the CHSB staff on the evaluation of the proposed equipment, software, and/or services.

3.2 A letter of support from a CJIS user agency detailing the potential benefits of the proposed product(s).

3.3 A report which details the technical scope of the equipment/software/services to be provided to the end user. For hardware and software, this must include a detailed list of CJIS functionality expected to be provided, and specific details about the method to be used in order to maintain a high level of security within the network at all times.

3.4 A report containing detailed specifications for the equipment to be connected, including proposed configurations.

3.5 A detailed narrative of the benefits which will be provided to the end users by the proposed equipment or software.

3.6 A written explanation of how the vendor intends to ensure the long- term viability of the proposed equipment/software and/or services as the CJIS network and systems evolve and change over time.

3.7 A detailed description of how the vendor proposes to test the equipment within the CJIS network in accordance with these guidelines, including a description of how the user will have uninterrupted access to the CJIS during all testing.

3.8 A description of how the vendor intends to manage improvements in its systems after the initial implementation.

3.9 A description of how the vendor plans to provide maintenance services on any hardware/software to be connected to the CJIS network. Maintenance services are required for compliance with the agency user agreement.

3.10 A list of all personnel who will be working on the proposed project, including names, addresses, and dates of birth. The CHSB will perform criminal record checks on all such persons and reserves the right to deny access to the CJIS system if it deems an individual unsuitable based on the information obtained from this record check. A complete updated list will be submitted at least annually, and record checks will be conducted accordingly. In addition, and in accordance with 803

C.M.R. 3.02(3), all such vendor personnel shall be required to complete a fully executed Agreement of Non-Disclosure with each criminal justice agency to which services are being provided.

3.11 Provide a complete set of signed authorization and agreement forms as contained in Appendix A of this document.

Any changes in the technical scope of the system must be reviewed and approved by the CHSB prior to being implemented in the field. No functional changes in the technical scope of the system will be allowed after the initial technical scope has been approved without a revised technical scope and subsequent written approval from the CHSB. This provision applies to the system during all testing and after final approval.

4.0 Alpha Level Testing:

4.1 If the project is approved by the CHSB, the vendor will be required to select one Alpha test site, which test site will be subject to the approval of the CHSB. The CHSB will base its approval on that site's compliance with the CJIS User Agreement, and that site's history of working with the CHSB. The CHSB will work with the vendor to develop a time period during which alpha testing shall occur.

4.2 After review and acceptance of the alpha test site, the vendor will then be approved to work with the test site to implement the system as approved by the CHSB. The CHSB will designate a primary contact person to work with the vendor during this phase of the project to provide technical assistance when required, to conduct spot audits of the vendor's use of the system, and to report on the progress of the implementation. The CHSB reserves the right to terminate the Alpha testing at any time, and termination may occur under conditions including, but not limited to, the following :

4.2.1 the CHSB determines that the testing is interfering with the normal operations of the CJIS system or network;

4.2.2 the CHSB determines that the vendor is in violation of any provision of these guidelines;

4.2.3 the CHSB determines that the vendor is not performing its testing in accordance with the approved technical scope;

4.2.4 the user agency requests that the CHSB suspend testing activities;

4.2.5 the CHSB determines that the vendor is utilizing the CJIS system in an inappropriate way, or in such a way as to cause the user agency to be in violation of its CJIS user agreement;

4.2.6 the CHSB becomes aware of a problem in the approved technical scope which represents a possible or real breach of security, or which would otherwise jeopardize the proper functioning of the network.

4.3 The CHSB will provide specific guidelines for system use during all testing. This may involve the use of test or restricted network addresses or physical locations, during which time the CHSB may monitor the activities of the vendor to insure compliance with the approved technical specification and scope.

4.4 When the vendor has completed the test implementation as approved in the technical scope, the vendor will be required to schedule a demonstration with the CHSB. A full demonstration of the system is expected, and appropriate CHSB staff will make a determination of the system's full compliance with the approved technical scope.

4.5 Should the vendor fail to demonstrate the ability of the equipment/software to satisfy the functionality contained in the technical scope, the CHSB will work with the vendor and user agency to identify the problem areas. The vendor will be given an opportunity to continue testing in accordance with the provisions of this section for the purpose of bringing the system into full compliance. The vendor may then request an additional demonstration as outlined in 4.4 above. The CHSB will conduct a maximum of two (2) demonstration visits for the purpose of determining full compliance. After two (2) failed attempts, further evaluation will be at the discretion of the Executive Director.

5.0 Beta Level Testing:

5.1 After successful completion of the Alpha test, the vendor will be required to select a minimum of one, and a maximum of four additional test sites, which will be subject to the approval of the CHSB. The CHSB will base its approval on each site's compliance with the user agreement, and the site’s history of working with the CHSB. The CHSB will work with the vendor to develop a time period during which beta testing shall occur.

5.2 After review and acceptance of each beta test site, the vendor will then be approved to work with the test sites to implement the system as approved by the CHSB. The CHSB will designate a primary contact person to work with the vendor during this phase of the project to provide technical assistance when required, to conduct spot audits of the vendor's use of the system, and to report on the progress of the implementation. The CHSB reserves the right to terminate the beta testing at any time, and termination may occur under conditions including, but not limited to, the following :

5.2.1 the CHSB determines that the testing is interfering with the normal operation of the CJIS system or network;

5.2.2 the CHSB determines that the vendor is in violation of any provision of these guidelines;

5.2.3 the CHSB determines that the vendor is not performing its testing in accordance with the approved technical scope;

5.2.4 the user agency requests that the CHSB suspend testing activities;

5.2.5 the CHSB determines that the vendor is utilizing the CJIS system in an inappropriate way, or in such a way as to cause the user agency to be in violation of its CJIS user agreement;

5.2.6 the CHSB becomes aware of a problem in the approved technical scope which represents a possible or real breach of security, or which would otherwise jeopardize the proper functioning of the network.

5.3 The CHSB will provide specific guidelines for use during all testing. This may involve the use of test or restricted network addresses or physical locations, during which time the CHSB may monitor the activities of the vendor to insure compliance with the approved technical specification and scope.

5.4 When the vendor has completed the implementation at each test site as approved in the technical scope, the vendor will be required to notify the CHSB. The CHSB may require a full demonstration of the system at all or at selected beta test sites. CHSB staff will make a determination of the system's full compliance with the approved technical scope.

5.5 Should the vendor fail to demonstrate the ability of the equipment/software to satisfy the functionality contained in the technical scope, the CHSB will work with the vendor and user agency to identify the problem areas. The vendor will be given an opportunity to continue testing in accordance with the provisions of this section for the purpose of bringing the system into full compliance. The vendor may then request an additional demonstration as outlined in 5.4 above. The CHSB will conduct a maximum of two (2) demonstration visits for the purpose of determining full compliance. After two (2) failed attempts, further evaluation will be at the discretion of the Executive Director.

6.0 Final Approval - Ongoing Oversight / Reporting

6.1 After completing the final review of the beta test sites as outlined in section 5 above, the CHSB will make a determination as to whether or not the system is in compliance with agency policies, and that it functions properly in the current technical environment.

6.2 If it is found to be in compliance, the vendor will be authorized to offer the approved system to additional user sites in accordance with the approved technical scope without further approval from the CHSB.

6.3 The CHSB will not provide an endorsement for the use of the vendor's products, but will provide a statement of compliance with current agency technologies and policies.

6.4 So as to not to violate Section IV (D) of the CJIS user agreement, a criminal justice agency seeking to make use of a vendor's "non-standard" product must sign an amendment to said user agreement. This amendment must be signed prior to the installation of the vendor's products on the CJIS network.

6.5 Even after the system has been approved for general use, the provisions of section 3.10 shall apply. When the vendor wishes to make improvements or changes in the way the system operates, a revised technical scope must be submitted to the CHSB for review prior to implementation. The CHSB may, at its sole discretion, approve the changes for immediate implementation without further review, may require an informal technical review/demonstration of the function(s) prior to implementation, or may, if the changes appear significant enough, require a formal Alpha/Beta test as outlined in sections 4 and 5 above.

6.6 The CHSB is not responsible for any impact that changes to the CJIS system may have on vendor systems approved under these guidelines. The responsibility for insuring the long term viability of systems is the vendor's alone. Where feasible, the CHSB will attempt to work with vendors to keep them informed of potential changes and to help them understand technical changes as they are implemented.

6.7 When changes occur in vendor personnel working with the CJIS system, a revised list, as required by section 3.11, must be submitted to the CHSB prior to those persons having access to any equipment connected to the CJIS system. As outlined in section 3.11, the CHSB will perform criminal record checks on all persons on this list, and reserves the right to deny access to the CJIS system if it deems an individual unsuitable based on the information obtained from this record check.

6.8 Vendors are required to report certain information to the CHSB on an annual basis. The following information must be provided to the Executive Director by January 15th , of each calendar year:

6.8.1 A list of all user agencies (Clients) currently utilizing the equipment/software approved under these guidelines;

6.8.2 A list of agencies that the vendor believes may be currently considering the purchase of the vendor's product(s). This information will be used by the CHSB for planning purposes only and will not be disclosed by the agency in any way;

6.8.3 Any updates to the information provided in sections 3.1, 3.4, 3.6, 3.7, 3.8, and 3.9;

6.8.4 A complete list of all vendor personnel who are currently working on the proposed project, including names, addresses, and dates of birth. A criminal record check will be performed on all personnel at least annually.

6.9 The CHSB may conduct spot audits and site visits to insure that the functionality being provided by the installed system(s) is in compliance with the currently approved technical scope, and to verify that all provisions of these guidelines are being met. Systems found to be out of compliance shall be subject to suspension of service, in addition to any and all sanctions that may be imposed by the CHSB pursuant to the terms and conditions of the user agreement. In addition, if systems are found to be out of compliance, the CHSB reserves the right to reject future user agreement amendments that would allow the use of the product(s) in question. Furthermore, if systems are found to be out of compliance, the CHSB reserves the right to terminate any further testing, and/or revoke the vendor's privileges to work with the CHSB on future projects.

Appendix A

Authorization and Agreements Required

Individual Agreement of Non-Disclosure

Criminal Offender Record Information ("CORI")

Individual Agreement of Non-Disclosure

I, _____, acknowledge that I have read and understand the provisions of Massachusetts General Laws, c. 6, §§ 167-178B, of which sections 177-178 provide that it is a criminal offense to willfully disclose to any unauthorized person or agency any criminal offender record information concerning an individual or to willfully falsify any criminal offender record information. Unauthorized access to or dissemination of criminal offender record information is punishable by a fine of not more that five thousand dollars ($5,000.00), or imprisonment in jail or house of correction for not more than one year, or both. Any such dissemination also subjects me to a suit for civil damages and/or a civil fine of up to five hundred dollars ($500.00) for each such willful violation.

I also understand that a criminal record check will be conducted on me by the Criminal History Systems Board as a prerequisite to my having authorization for access to CORI.

Signed this _____ day of _____ , 200___ .

_____
Signature

_____ _____ _____
Last name First name Middle initial

_____ _____
Maiden name Alias

_____ _____
Date of Birth (MM/DD/YY) Social Security Number (requested but not required)

_____
Job title

_____
Agency/ Business

_____
Address

This document is to be completed by ALL persons employed by, contracted with, or otherwise operating in association with the herein named agency, and who may have access to CORI.